CNET Networks

Security and Privacy

From Carnivore to Palladium

10/12/2002

Dan Farber
VP Editorial
CNET Networks

The Climate

- Almost half of those surveyed said they think the First Amendment goes too far in the rights it guarantees.
- The least popular First Amendment right is freedom of the press.
- More than 40 percent of those polled said newspapers should not be allowed to freely criticize the U.S. military's strategy and performance.
- More than four in 10 said they would limit the academic freedom of professors and bar criticism of government military."

SOURCE: American Journalism Review, September 2002

The climate

- A year after 9/11 more than two-thirds of Americans believe the government should be granted wide privileges in deciding what information to post on government agency web sites and what information to keep off for fear it will help terrorists
  - For example the Nuclear Regulatory Commission took down its site
  - U.S. Geological Survey removed some reports on water resources
- But a majority of those surveyed don't believe such action will make a significant difference in battling terrorists
- The respondents were equally divided for and against monitoring email and online activities of individuals and organizations

Source: Pew Internet and American Life Project, July 02

The climate

- New technologies enable easier, ubiquitous surveillance within and outside an enterprise.
  - Xerox tested a system that gave each employee an electronic transponder, which triggered sensors installed throughout its Palo Alto Research Center campus so that security managers could track the movements of each employee at all times.
- Police in Tampa, Florida, and other cities have set up video cameras in various locations and used face-recognition technology to try to match video images to a database of known criminals.
- Operation Thumbs Up: Police in Arlington, Texas are asking businesses to voluntarily participate in a program to take customers' fingerprints if they pay by check.

Patriot Act: Times have changed

- **Sneak and Peek**
- In *Wilson v. Arkansas*, 514 U.S. 927 (1995), and *Richards v. Wisconsin*, 520 U.S. 385 (1997), the Supreme Court held that contemporaneous notice was normally constitutionally required, and could be dispensed with only under exceptional circumstances.
- The Patriot Act: Section 213 amended section 3103a of Title 18, United States Code, allows the FBI to secretly access information, without notice. In the case of individuals who are not prosecuted—those where the likelihood of government overreaching is the greatest—notice is never given.
- The Foreign Intelligence Surveillance Act (FISA) authorizes the FBI to conduct electronic surveillance and clandestine searches without full probable cause to believe that a crime has been or is about to be committed.

Patriot Act

- Sneak and peek is applied by the Patriot Act to the homes of citizens as well as to drug cases, tax fraud, providing false information on student loan applications, or any other federal crime.
- Under the Patriot Act, the FBI access the entire database of a credit card company and public library records, as well as records from banks, hotels, hospitals, retailers and universities with a claim that the information is "sought for" an investigation to protect against international terrorism or clandestine intelligence activities.
- Section 203 of the 2001 Patriot Act CIA agents working with law enforcement officers can now jointly draw up subpoenas, obtain the results of grand jury inquiries
- Sharing of information from intelligence investigations with criminal investigations allowed due to lower threshold for warrants in intelligence gathering
-

Practical Application: Expanded surveillance powers

- FBI made errors in 75 applications for wiretaps and electronic surveillance, mostly during Clinton administration
- In 2000 the FBI illegally videotaped suspects, improperly recorded telephone calls and intercepted e-mails without court permission in more than a dozen secret terrorism and intelligence investigations.
- Circumvents Fourth Amendment protections against unreasonable searches

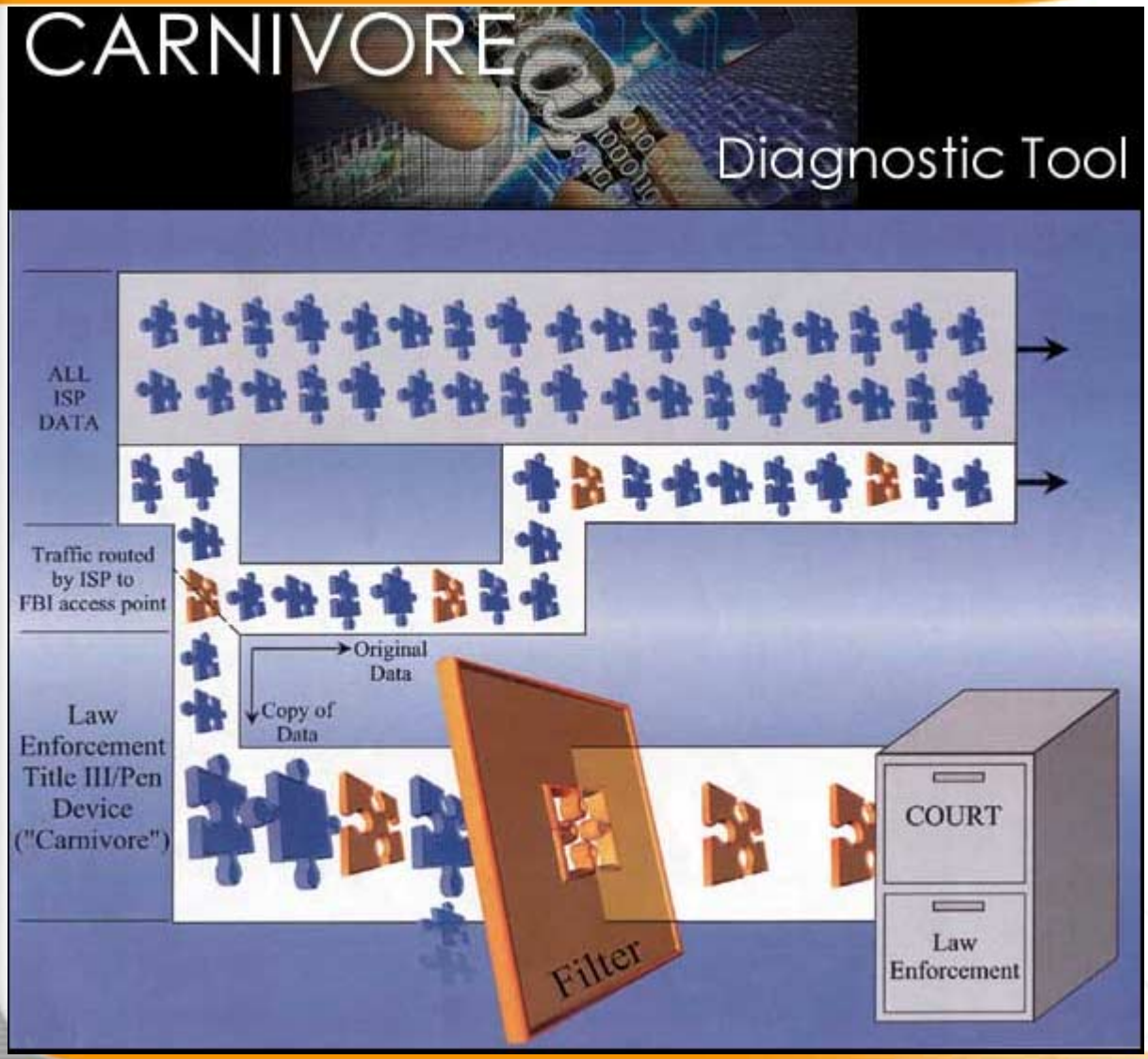
TIPS: Spying on your neighbors?

- As originally conceived, TIPS would enlist over 20 million citizen spies who would report on the suspicious behavior of their neighbors.
- The initial plan, and a 10-city test involving some 1 million citizen spies set for this month, was scrapped
- A battle is shaping up in Congress over efforts to block funding for the TIPS program entirely.
  - Last month, the House passed its version of the Homeland Security bill with a measure added by Majority Leader Dick Armey, R-Texas, that prohibited federal funding for programs that would have American citizens spying on each other.
  - Sen. Pat Leahy, D-Vt., is advocating a similar proposal in the Senate's version of the bill, but was stymied by Senate Government Operations Committee Chair Sen. Joe Lieberman, D-Conn.
  - Private agencies have been approached to run a modified version of the original TIPS

Digital Monitoring and Filtering

- **United States**
  - Carnivore: an automated system that plugs into an ISP to record activity
- **UK**
  - Echelon: automated global interception and relay system
    - Developed under US/UK Agreement of 1947 with US-NSA, UK, Canada, Australia & New Zealand
- **Russia**
  - Federal Security Service: Monitors Internet transmissions in and out of Russia
  - Federal Agency for Government Communications and Information
- **China**
  - “Computer Information Network and Internet Security, Protection and Management Regulations," issued by the Ministry of Public Security.

Carnivore



HOW IT WORKS

- Carnivore, also known as DCS1000 is a specialized network sniffer that intercepts and stores packets based on criteria set by the court order.
- It gives the FBI direct access to Internet Service Provider (ISP) data networks
- Some ISPs have this capability, such intercepting an individuals e-mail to and from a specific party
- Also keyboard loggers used to gain information

Carnivore: Powerful, Clunky, Defective

- EPIC (Electronic Privacy Information Center sued the FBI under FOIA to get information on how Carnivore was being used
- FBI documentation recounted how Carnivore failed to work properly, and even disrupted a UBL anti-terror investigation under FISA (Foreign Intelligence Surveillance Act) in March 2000
- Carnivore captured e-mail on individuals not covered by the court order, a violation of federal wiretap law
- The over collection problem leads to contaminated evidence

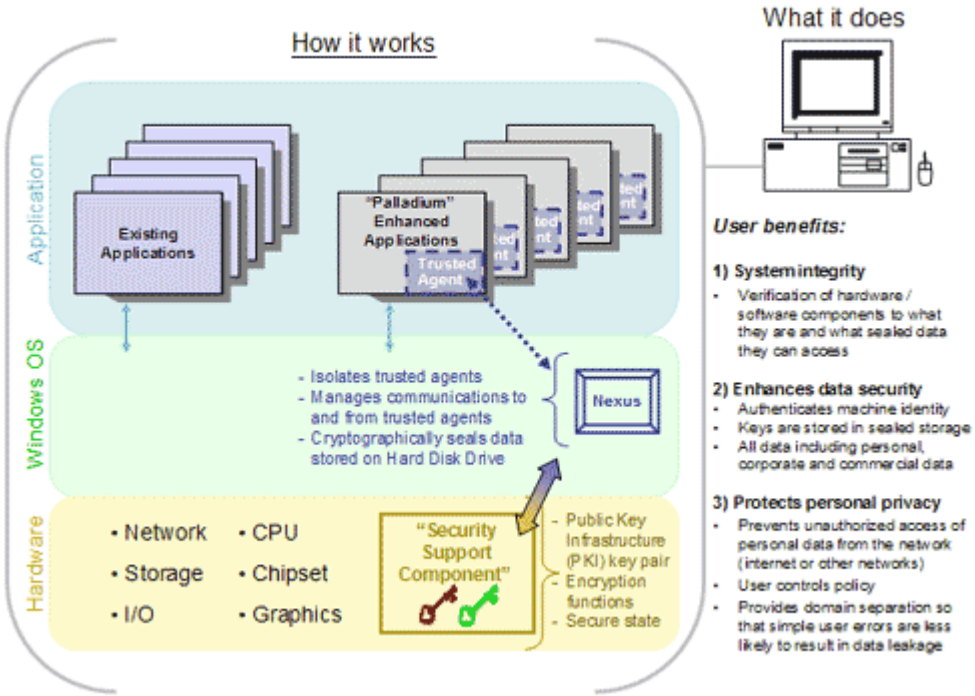
Trusted Computing Platform Alliance (TCPA)

- Baseline hardware capabilities
- Improved traditional security features
- Persistent storage of confidential information
- Platform authentication
- Random number generator
- New security capabilities
- Anonymous/multiple identities
- Integrity metrics
- Exportable worldwide
- Excludes general purpose encryption
- Owner has complete control of policy
- Opt in - Owner decides if and when to

Security and Technology

- Microsoft
  - Proposes a hardware/software combination integrated with Windows

The technology can dramatically enhance privacy and enable secure, authenticated transactions without disclosure of a consumer's identity, but paves the way for complete digital rights management solutions.



Security and Technology

- **Intel**
  - Lagrande technology will protect data in a kind of vault as soon as it enters a PC, preventing it from being accessed by hackers. LT also establishes secure pathways to safeguard data as it enters, moves through, and is stored on a system.
- **Industry**
  - **Smart cards**
  - **Biometrics**

Privacy and Identity in Cyberspace

Your Info/Identity

1. Name
2. Signature
3. SSI
4. Description
5. Address
6. Phone number
7. Passport
8. Education
9. Employment history
10. Bank account
11. Credit card
12. Driver's liscence
13. Insurance

Legislative Action

- Privacy Policies
- Disposal of personal information
- Spam

Connected World

Core and Networking 2005 — 2012

Broadband plus wireless LANs drives hot spots and innovative form factors

Integrated IP network infrastructure dominates communications

Seamless local vs. centralized storage and access

RFID chips embedded in objects (and people?)

Embedded devices networked

Gartner

Managing context in a mobile world

Mobility and Physical World
2005 — 2012

Instant access to e-services from any location

Alternate power sources commercialized for mobile devices: fuel cells, kinetic power

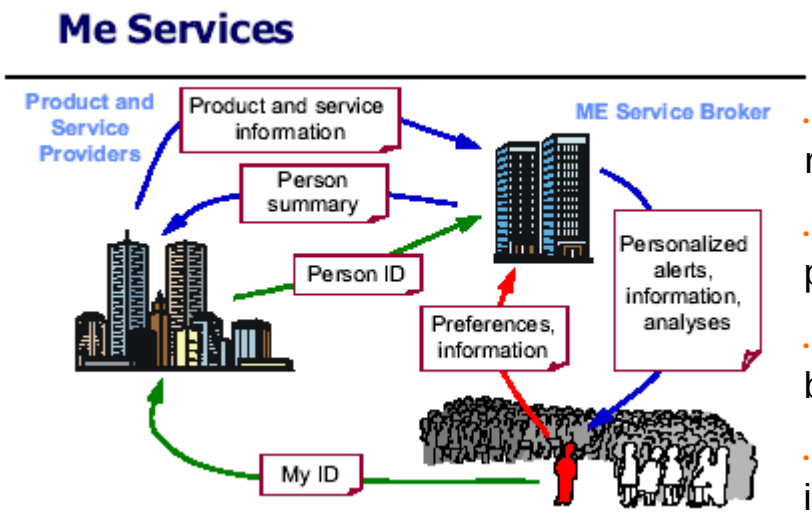
Location-based and context-aware services broadly adopted

Physical objects coded and uniquely identifiable

Cashless micropayments build on current payment infrastructures

- Personal mobile or wearable devices.
- Alternate power sources such as fuel cells
- Location-based and context aware services that take advantage of physical location and assumed interests and goals
- Semantic coding/tags, which build on top of the physical tags to provide an (ideally) universal reference standard for uniquely identifying items and their properties.
- Applications such as electronic wallets, although the physical presence of the mobile or wearable device may not be required

Trust Service Brokers



- Record personal information, preferences and rules that allow systems to deduce roles.
- Provide selected personal information to third parties on receipt of a user ID.
- Filter information and events from third parties based on user roles and needs.
- Most likely to be managed by financial institutions, such as banks, in combination with industry standard identity services such as Passport or Liberty

Do the current laws apply?

- **Privacy:** Legal controls on the use of mobile phone-location information.
- **Liability:** Product and, in the future, service liability will apply to personal devices and eventually applications requiring “over the air” upgrades of systems.
- **Law enforcement:** Technologies such messaging provide communications channels outside state control. Mobile devices pose new crime opportunities.
- **Legislation in an e-world:** Much existing legislation implicitly assumes that it applies to a traditional physical world. For example, jurisdiction applies in a fixed region (such as a country or town), and laws deal with measurable issues, such as working hours. The future Net world changes the foundations on which some of these laws are built. People move while conducting transactions, work and leisure are not clearly bounded and so on.
- **Financial issues:** Issues such as taxation and economic policy are impacted by micro-payments, e-cash and virtual currencies. New monopolists (such as the telcos left standing) may need to be controlled.
- **E-government:** Mass adoption of computing devices offers new e-government channels.

Source: Gartner

The Future?